

FirstNet RFP outlines financial penalties for contractor, if public-safety adoption targets are missed

Urgent Communications By Donny Jackson

January 15, 2016

If at least 70% of the targeted public-safety users do not subscribe to the [FirstNet](#) system in a given year upon its operational completion, the FirstNet contractor could pay more than \$100 million in financial penalties and risk losing control of certain business functions, according to the FirstNet request for proposal (RFP).

Building and operating a nationwide broadband network to meet the needs of public safety is the primary purpose of FirstNet, but public-safety users are not required to adopt the FirstNet system. Thus, the FirstNet offering needs to be attractive enough from the performance and financial standpoints to convince public safety to subscribe to the network.

In addition, the selected contractor also is allowed to sell wireless services to traditional consumer customers—on a secondary basis, behind public-safety prioritized traffic—while utilizing FirstNet spectrum. To ensure that the contractor does not use the FirstNet spectrum simply to pursue commercial subscribers, FirstNet officials said the RFP would include measures that would penalize a contractor that did not meet public-safety adoption goals.

Those measures were revealed when FirstNet released the RFP on Wednesday. When the FirstNet system reaches the Final Operational Capability (FOC) stage—something that is expected to occur five years after the contract is signed—the contractor will have to demonstrate that it has met the public-safety adoption goals or pay a financial penalty, known as a “disincentive payment.”

If the contractor fails to reach more than 70% of its public-safety adoption goal for a state or territory, it would have to pay 100% of its maximum disincentive payment—nationwide, a figure that ranges from \$124.7 million to \$178.3 million, increasing annually over a 20-year period—for jurisdiction for that particular year. A 90% public-safety adoption rate would result in the contractor paying FirstNet 15% of the maximum disincentive payment, while an 80% public-safety adoption rate would result in a payment of 44% of the maximum disincentive payment.

In addition, failure to meet the public-safety adoption goals exposes the contractor to a variety of remediation efforts by FirstNet, including FirstNet recommending lower pricing or taking certain business functions from the contractor—with the contractor funding any replacement operations.

However, FirstNet does not dictate what those public-safety adoption goals will be in its RFP. Instead, it will allow bidders to propose what the public-safety adoption rate should be. In selecting the winning contractor, the evaluation team will consider the proposed public-safety adoption targets proposed by each bidder.

Exactly who is a public-safety user is not delineated by FirstNet in the RFP, even though the definition of a “public-safety entity” (PSE) that can be prioritized on the network was a topic of two separate public-notice proceedings. The RFP merely states that public-safety entities are defined in FirstNet’s enabling legislation, but it provides a level of distinction on the matter in association with the disincentive-payment process.

“For the purpose of this disincentive mechanism, FirstNet further delineates PSEs into two user groups: a primary user group and extended primary user group,” the RFP states. “FirstNet prefers device connections from the primary user group, which consists of law enforcement, fire, and emergency medical services users.

“The Contractor is also encouraged to drive customer adoption and use of the [FirstNet system] through the extended primary user group, which consists of all other public safety users, as defined in the Act. The Contractor will be subject to disincentive payments upon failure to achieve 100% of the proposed connection targets for either user group.”

If at least 70% of the targeted public-safety users do not subscribe to the [FirstNet](#) system in a given year upon its operational completion, the FirstNet contractor could pay more than \$100 million in financial penalties and risk losing control of certain business functions, according to the FirstNet request for proposal (RFP).

Building and operating a nationwide broadband network to meet the needs of public safety is

the primary purpose of FirstNet, but public-safety users are not required to adopt the FirstNet system. Thus, the FirstNet offering needs to be attractive enough from the performance and financial standpoints to convince public safety to subscribe to the network.

In addition, the selected contractor also is allowed to sell wireless services to traditional consumer customers—on a secondary basis, behind public-safety prioritized traffic—while utilizing FirstNet spectrum. To ensure that the contractor does not use the FirstNet spectrum simply to pursue commercial subscribers, FirstNet officials said the RFP would include measures that would penalize a contractor that did not meet public-safety adoption goals.

Those measures were revealed when FirstNet released the RFP on Wednesday. When the FirstNet system reaches the Final Operational Capability (FOC) stage—something that is expected to occur five years after the contract is signed—the contractor will have to demonstrate that it has met the public-safety adoption goals or pay a financial penalty, known as a “disincentive payment.”

If the contractor fails to reach more than 70% of its public-safety adoption goal for a state or territory, it would have to pay 100% of its maximum disincentive payment—nationwide, a figure that ranges from \$124.7 million to \$178.3 million, increasing annually over a 20-year period—for jurisdiction for that particular year. A 90% public-safety adoption rate would result in the contractor paying FirstNet 15% of the maximum disincentive payment, while an 80% public-safety adoption rate would result in a payment of 44% of the maximum disincentive payment.

In addition, failure to meet the public-safety adoption goals exposes the contractor to a variety of remediation efforts by FirstNet, including FirstNet recommending lower pricing or taking certain business functions from the contractor—with the contractor funding any replacement operations.

However, FirstNet does not dictate what those public-safety adoption goals will be in its RFP. Instead, it will allow bidders to propose what the public-safety adoption rate should be. In selecting the winning contractor, the evaluation team will consider the proposed public-safety adoption targets proposed by each bidder.

Exactly who is a public-safety user is not delineated by FirstNet in the RFP, even though the definition of a “public-safety entity” (PSE) that can be prioritized on the network was a topic of two separate public-notice proceedings. The RFP merely states that public-safety entities are defined in FirstNet’s enabling legislation, but it provides a level of distinction on the matter in association with the disincentive-payment process.

“For the purpose of this disincentive mechanism, FirstNet further delineates PSEs into two user groups: a primary user group and extended primary user group,” the RFP states. “FirstNet prefers device connections from the primary user group, which consists of law enforcement, fire, and emergency medical services users.

“The Contractor is also encouraged to drive customer adoption and use of the [FirstNet system] through the extended primary user group, which consists of all other public safety users, as defined in the Act. The Contractor will be subject to disincentive payments upon failure to achieve 100% of the proposed connection targets for either user group.”

If at least 70% of the targeted public-safety users do not subscribe to the [FirstNet](#) system in a given year upon its operational completion, the FirstNet contractor could pay more than \$100 million in financial penalties and risk losing control of certain business functions, according to the FirstNet request for proposal (RFP).

Building and operating a nationwide broadband network to meet the needs of public safety is the primary purpose of FirstNet, but public-safety users are not required to adopt the FirstNet system. Thus, the FirstNet offering needs to be attractive enough from the performance and financial standpoints to convince public safety to subscribe to the network.

In addition, the selected contractor also is allowed to sell wireless services to traditional consumer customers—on a secondary basis, behind public-safety prioritized traffic—while utilizing FirstNet spectrum. To ensure that the contractor does not use the FirstNet spectrum simply to pursue commercial subscribers, FirstNet officials said the RFP would include measures that would penalize a contractor that did not meet public-safety adoption goals.

Those measures were revealed when FirstNet released the RFP on Wednesday. When the FirstNet system reaches the Final Operational Capability (FOC) stage—something that is

expected to occur five years after the contract is signed—the contractor will have to demonstrate that it has met the public-safety adoption goals or pay a financial penalty, known as a “disincentive payment.”

If the contractor fails to reach more than 70% of its public-safety adoption goal for a state or territory, it would have to pay 100% of its maximum disincentive payment—nationwide, a figure that ranges from \$124.7 million to \$178.3 million, increasing annually over a 20-year period—for jurisdiction for that particular year. A 90% public-safety adoption rate would result in the contractor paying FirstNet 15% of the maximum disincentive payment, while an 80% public-safety adoption rate would result in a payment of 44% of the maximum disincentive payment.

In addition, failure to meet the public-safety adoption goals exposes the contractor to a variety of remediation efforts by FirstNet, including FirstNet recommending lower pricing or taking certain business functions from the contractor—with the contractor funding any replacement operations.

However, FirstNet does not dictate what those public-safety adoption goals will be in its RFP. Instead, it will allow bidders to propose what the public-safety adoption rate should be. In selecting the winning contractor, the evaluation team will consider the proposed public-safety adoption targets proposed by each bidder.

Exactly who is a public-safety user is not delineated by FirstNet in the RFP, even though the definition of a “public-safety entity” (PSE) that can be prioritized on the network was a topic of two separate public-notice proceedings. The RFP merely states that public-safety entities are defined in FirstNet’s enabling legislation, but it provides a level of distinction on the matter in association with the disincentive-payment process.

“For the purpose of this disincentive mechanism, FirstNet further delineates PSEs into two user groups: a primary user group and extended primary user group,” the RFP states. “FirstNet prefers device connections from the primary user group, which consists of law enforcement, fire, and emergency medical services users.

“The Contractor is also encouraged to drive customer adoption and use of the [FirstNet system]

through the extended primary user group, which consists of all other public safety users, as defined in the Act. The Contractor will be subject to disincentive payments upon failure to achieve 100% of the proposed connection targets for either user group.”

Providing communications to the primary user group of fire, EMS and law enforcement has been the expected focus of the [FirstNet](#) since its conception, there has been considerable industry debate about the manner in which traffic the extended primary user group—for instance, utilities, governments, healthcare entities and transportation providers—should be treated on the network.

Prioritization and preemption issues are not addressed in the RFP, other than the requirement that such functionality must be included in the network. Details about how that will work operationally are still being formulated.

Whether the contractor meets its public-safety adoption goals is based on the number of device connections utilized by public-safety users.

“For the purposes of this disincentive mechanism, FirstNet defines a device connection as a device on a post-paid contract with an eligible NPSBN user that has been generating billable revenue for three consecutive months. Each device connection will be assigned to the state or territory based on the registered billing address of that device connection. The connection targets will serve as the basis for the disincentive mechanism structure further described below.”

FirstNet officials have estimated that there are 4 million to 12 million public-safety users in the U.S., depending on how broadly the public-safety-entity definition is interpreted.

One potential complication in this formula is the use of Internet of Things (IoT) devices, such as sensors and wearables. For instance, a first responder in the field could utilize several different devices at an incident scene, but each of the devices could utilize separate connections or the data traffic could be aggregated via a wearable gateway and be transmitted over a single connection. How those devices are calculated could impact whether the contractor has to pay a disincentive penalty.

Another potential complication cited by some industry sources is the growth of cybercrime and cyberattacks, which introduces the possibility of a potential new wave of public-safety users—for instance, key security personnel in data centers—that may not have been considered part of public safety under a traditional definition but may be relevant today.

[Link to Article](#)

[Link to Urgent Communications News Articles](#)